Amendments to the Claims

The listing of claims will replace all prior versions, and listings of claims in the application.

1. (Currently Amended) A method for determining whether a client is attempting to copy an application or use the application without authorization, the method comprising:

creating data for at least one prediction log file for the application;

forwarding the at least one prediction log file to a prediction server;

based on said at least one prediction log file, determining prediction knowledge for the application, wherein said prediction knowledge is indicative of authorized use of the application and wherein said prediction knowledge is stored in a prediction file;

forwarding said prediction file to the client executing the application; and

using said prediction file to detect abnormalities and determine whether the client is attempting to copy the application or use the application without authorization.

2. (Original) The method of claim 1, further comprising:

if it is determined that the client is attempting to access the application without authorization, then terminating the client's access to the application.

3. (Currently Amended) The method of claim 1, wherein the step of creating ~~is comprised of the following~~ comprises:

merging block IDs;

creating short term strings;

deleting triggers;

creating long term strings;

sorting said short term strings and said long term strings; and

creating the triggers scheme data structure to create said at least one prediction log file.

4. (Currently Amended) The method of claim 3, wherein the step of merging block IDs ~~is comprised of the following~~ comprises:

gathering at least one record in a connection table, wherein said at least one record has a first ID key and an second ID key;

sorting said gathered records by said second ID key, wherein said second ID key in said sorted records is sorted by average distance ascending; and

merging said gathered records with said first ID key and said second ID key with records with said second ID key and a third ID key to create records with said first ID key and said third ID key.

5. (Currently Amended) The method of claim 1, wherein the step of using said prediction file ~~is comprised of the following~~ comprises:

using said prediction file to determine pairs of block IDs that are most likely to be accessed together, wherein said pairs of block IDs has a first ID block and a second ID block;

when the client accesses said first ID block, then starting a counter of D block requests; and

after D block requests if the client has not accessed said second ID block, then indicating that the client is attempting to copy the application or use the application without authorization.

6. (Currently Amended) A system for determining whether a client is attempting to copy an application or use the application without authorization, the method comprising:

~~means for creating~~ a module to create data for at least one prediction log file for the application;

a module to forward the at least one prediction log file to a prediction server;

~~based on said at least one prediction log file, means for determining~~ a module to determine prediction knowledge for the application based on said at least one prediction log file, wherein said prediction knowledge is indicative of authorized use of the application and wherein said prediction knowledge is stored in a prediction file;

~~means for forwarding~~ a module to forward said prediction file to the client executing the application; and

~~means for using~~ a module to use said prediction file to detect abnormalities and determine whether the client is attempting to copy the application or use the application without authorization.

7. (Currently Amended) The system of claim 6, further comprising:

~~means for terminating~~ a module to terminate the client's access to the application if it is determined that the client is attempting to access the application without authorization.

8. (Currently Amended) The system of claim 6, wherein the ~~means for creating is comprised of the following~~ the module for creating comprises at least one of:

means for merging block IDs;

means for creating short term strings;

means for deleting triggers;

means for creating long term strings;

means for sorting said short term strings and said long term strings; and

means for creating the triggers scheme data structure to create said at least one prediction log file.

9. (Currently Amended) The system of claim 8, wherein the means for merging block IDs ~~is comprised of the following~~ comprises:

means for gathering at least one record in a connection table, wherein said at least one record has a first ID key and an second ID key;

means for sorting said gathered records by said second ID key, wherein said second ID key in said sorted records is sorted by average distance ascending; and

means for merging said gathered records with said first ID key and said second ID key with records with said second ID key and a third ID key to create records with said first ID key and said third ID key.

10. (Currently Amended) The system of claim 6, wherein the ~~means for using~~ module for using said prediction file ~~is comprised of the following~~ comprises:

means for using said prediction file to determine pairs of block IDs that are most likely to be accessed together, wherein said pairs of block IDs has a first ID block and a second ID block;

means for starting a counter of D block requests when the client accesses said first ID block; and

means for indicating that the client is attempting to copy the application or use the application without authorization after D block requests if the client has not accessed said second ID block.

11. (New) A client based method for determining whether a client is attempting to copy an application or use the application without authorization, the method comprising:

creating data for at least one prediction log file for the application;

forwarding the prediction log file to a prediction server, wherein the prediction server (i) receives prediction log file, (ii) determines prediction knowledge for the application based the prediction log file, and (iii) stores the prediction knowledge in a prediction file, said prediction file being indicative of authorized use of the application;

receiving the prediction file at the client executing the application; and

using said prediction file to detect abnormalities and determine whether the client is attempting to copy the application or use the application without authorization.

12. (New) The method of claim 11, wherein the client's access to the application is terminated if it is determined that the client is attempting to access the application without authorization.

13. (New) The method of claim 11, wherein the step of creating comprises:

merging block IDs;

creating short term strings;

deleting triggers;

creating long term strings;

sorting said short term strings and said long term strings; and

creating the triggers scheme data structure to create said at least one prediction log file.

14. (New) The method of claim 13, wherein the step of merging block IDs comprises:

gathering at least one record in a connection table, wherein said at least one record has a first ID key and an second ID key;

sorting said gathered records by said second ID key, wherein said second ID key in said sorted records is sorted by average distance ascending; and

merging said gathered records with said first ID key and said second ID key with records with said second ID key and a third ID key to create records with said first ID key and said third ID key.

15. (New) The method of claim 11, wherein the step of using said prediction file comprises:

using said prediction file to determine pairs of block IDs that are most likely to be accessed together, wherein said pairs of block IDs has a first ID block and a second ID block;

when the client accesses said first ID block, then starting a counter of D block requests; and

after D block requests if the client has not accessed said second ID block, then indicating that the client is attempting to copy the application or use the application without authorization.

16. (New) A server based method for determining whether a client is attempting to copy an application or use the application without authorization, the method comprising:

receiving at a prediction server a prediction log file for the application;

determining prediction knowledge for the application based on the prediction log file said prediction knowledge being indicative of authorized use of the application;

forwarding said prediction knowledge to the client executing the application, wherein the client uses said prediction knowledge to detect abnormalities and determine

whether the client is attempting to copy the application or use the application without authorization.

17. (New) The method of claim 16, wherein client's access to the application is terminated if it is determined that the client is attempting to access the application without authorization.

18. (New) The method of claim 16, wherein the prediction knowledge is created using a method comprising:

merging block IDs;

creating short term strings;

deleting triggers;

creating long term strings;

sorting said short term strings and said long term strings; and

creating the triggers scheme data structure to create said at least one prediction log file.

19. (New) The method of claim 18, wherein the step of merging block IDs is comprises:

gathering at least one record in a connection table, wherein said at least one record has a first ID key and an second ID key;

sorting said gathered records by said second ID key, wherein said second ID key in said sorted records is sorted by average distance ascending; and

merging said gathered records with said first ID key and said second ID key with records with said second ID key and a third ID key to create records with said first ID key and said third ID key.

20. (New) The method of claim 16, wherein the client executing the application performs the following steps:

using said prediction knowledge to determine pairs of block IDs that are most likely to be accessed together, wherein said pairs of block IDs has a first ID block and a second ID block;

when the client accesses said first ID block, then starting a counter of D block requests; and

after D block requests if the client has not accessed said second ID block, then indicating that the client is attempting to copy the application or use the application without authorization.